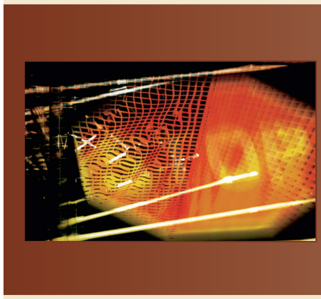
Replacing Lost or Stolen E-Passports

Jianming Yong, University of Southern Queensland
Elisa Bertino, Purdue University



The launch of e-passports raises concerns about how travelers can replace them if they're lost or stolen.

Until recently, border control had changed little over the years, despite advancing technology. Now, travelers routinely print out e-tickets from their computers, and many countries have started issuing e-passports with embedded biometric information. However, countries are taking different approaches to e-passports, raising concerns about how travelers can replace them in the event they're lost or stolen.

Travelers report the loss or theft of hundreds of thousands of passports each year. The Australian government estimates that 30,000 of the 1 million passports it issues annually are lost or stolen (http://foreignminister.gov.au/releases/2005/fa083_05.html), and in 2006, the United Kingdom reported that more than 290,000 passports were lost or stolen (http://press.homeoffice.gov.uk/press-releases/passport-warning?version=1).

E-PASSPORT INITIATIVES

In the wake of the 9/11 terrorist attacks, the US government launched a machine-readable passport (MRP) program to provide more secure border control. The next-generation passport that the US State Department began issuing in August 2006 features a contactless integrated circuit (IC) in the rear cover containing biographic data (name, date of birth, gender, place of birth, dates of passport issuance and expiration, and passport number) and a digital image of the bearer that authorities can use for facial-recognition comparisons.

Metallic material in the e-passport's front cover and spine is intended to prevent the chip from being skimmed or read when the passport is closed. Other security features include basic access-control technology, which requires electronic reading of the data page to unlock the chip; a randomized unique identification feature to reduce the chances of tracking; and an electronic signature to prevent data alteration and let authorities validate and authenticate the data.

The US is also pushing the 27 countries in its visa-waiver program to endorse e-passports. Such programs are now under way in most of those countries, but they're using a variety of approaches to the types of biometric information the passports contain, with some using only facial characteristics and others including fingerprints and iris scans.

Most e-passport projects or initiatives meet the International Civilization Aviation Organization's 2003 standards, which require the encoding of biometric information on a chip. Most countries also use radio frequency identification technology in their e-passports. However, chip-based e-passports have the same problem as conventional passports in authenticating the passport owner in the event the passport is stolen or lost.

TRADITIONAL PASSPORT PROCESS

A citizen applying for a traditional passport typically must provide documentation of his identity and submit an application to the passport authority, which verifies the submitted materials' accuracy from the passport repository. The authority then issues the passport and adds the information to the repository for archiving or monitoring.

Depending on the country, it can take from weeks to months to process a passport application. Even in urgent situations, securing a replacement passport can take several days. If a traveler's passport is lost or stolen, the traveler must appear in person at the passport authority to apply for a replacement, even though passport authorities aren't always nearby. For example, an overseas traveler could be visiting a country that doesn't have a passport authority. Without a passport, the traveler could find it difficult to enter the country where the passport authority is located. In the meantime, wrongdoers could use a passport for illicit purposes before it's reported lost or stolen.

E-PASSPORT MECHANISM

In addition to conventional identifiers, e-passports typically contain

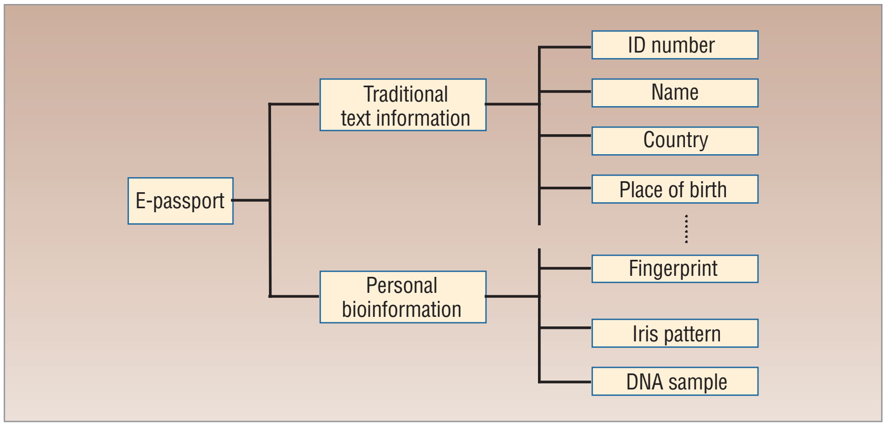


Figure 1. E-passport data structure. E-passports contain both traditional text information and personal biometric information.

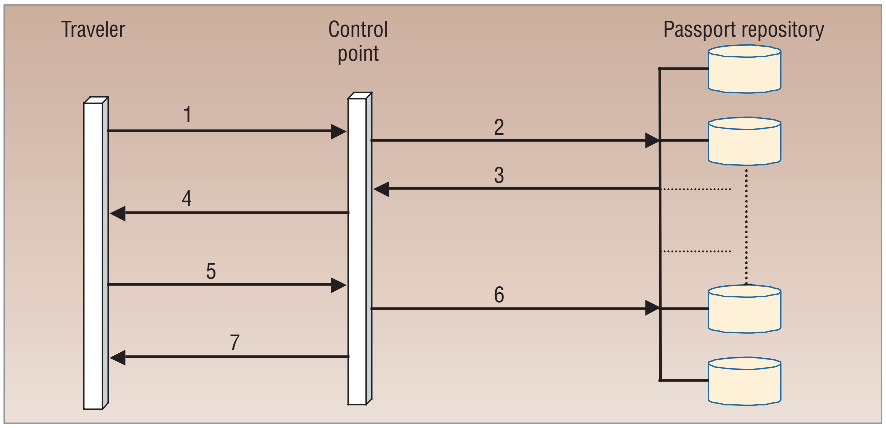


Figure 2. Verification with IC cards. The IC card is swiped at a control point, and the passport authority authenticates the request.

biometric information such as fingerprints, iris scans, or DNA samples. Passport authorities can collect the biometric information when citizens submit applications or appear for passport interviews. Because such data offers a unique means of personal identification, agencies could retrieve and match travelers' identities when they appear at border and customs checkpoints or airline check-in counters. Figure 1 illustrates the usual information structure of an e-passport.

Local passport repositories could store the information and allow only authorized parties to access it. Many passport authorities issue IC cards containing traditional text-based information, like age, nationality, height, gender, and so on. The IC cards don't need to contain biometric information because authorities could collect it on the spot. In fact, having the passport repository keep travelers' biometric information could effectively prevent IC card fraud.

Authorities could assign two numbers to IC cards: a difficult-to-remember 16-digit number displayed on the card and an easy-to-remember five-digit reference number. When travelers lose their IC cards, they could produce the reference number as one of their credentials.

Figure 2 illustrates how systems could verify travelers with IC cards using the following steps:

1. A traveler presents an IC card to swipe at the control point.
2. The control-point computer uses information on the IC card to connect to the correct passport repository.
3. The passport repository authenticates the request and replies with the traveler's biometric information.
4. Control-point officials let the traveler approach the bioreading device.
5. The system collects the traveler's biometric information and compares it with the biometric information from the passport repository.
6. The system reports the successful or failed verification to the passport repository for tracking.
7. If two sets of biometric information match, the traveler can proceed through the control point.

Figure 3 shows the verification process that authorities could use for travelers without IC cards. The process includes the following steps:

1. The traveler must enter text-based information, such as a passport, social security, or driver's license number.
2. The control point contacts the passport repository to retrieve the e-passport's text-based information.
3. The passport repository provides the requested information.
4. Control-point officials ask the traveler questions related to the text-based information.
5. If the traveler's answers match the retrieved information, the traveler's identity is initially recognized.
6. If the verification is successful, the control point contacts the passport repository again to get the traveler's biometric information.
7. The control point lets the traveler approach the bioreader.
8. The control point collects the biometric information and matches it with information received from the repository.
9. The system reports the successful or failed verification to the passport repository for tracking.
10. If the verification is successful, the traveler is allowed to pass through the control point.

It's clear from these verification-process scenarios that the Internet plays an important role for all transactions. Thus, e-passport systems will require robust network support.

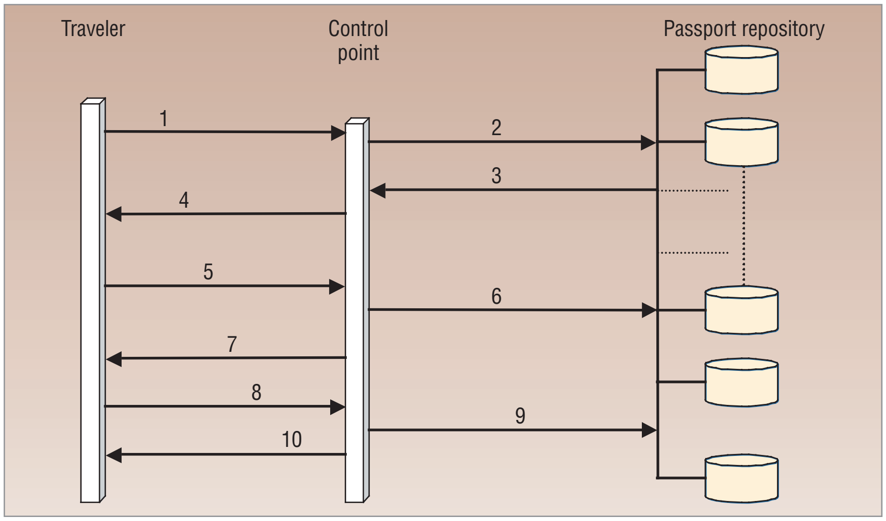


Figure 3. Verification without IC cards. The traveler enters credential information at the control point, which retrieves information from the passport repository.

NETWORK SUPPORT

The robust network needed to support an e-passport system must connect all border-control and customs checkpoints, airline check-in counters, passport authorities, and some government embassies and consulates. Such a network must meet a variety of requirements, including the following:

- *Security and privacy*. Because e-passport systems must transmit sensitive personal information, networks must have strong security and privacy techniques to ensure that malicious parties can't alter or eavesdrop on that information. We can easily anticipate that e-passport networks will become targets of a variety of attacks.
- *Accuracy.* E-passport systems must record information accurately when they collect, store, transfer, and verify travelers' digital identities.
- *Promptness*. The system should have a short response time for acquiring travelers' information. We estimate a one-minute maximum as an acceptable processing time for the control point to retrieve a traveler's information. Neither travelers nor control officers would accept a retrieval time of more than five minutes.
- *Availability.* The network infrastructure must work effectively around the clock and throughout the year. Control points must be able to reach passport repositories whenever the system needs the information. E-passport systems won't be viable if the system's availability isn't ensured.
- *Scalability.* Future expansion or reduction of e-passport nodes must not affect the performance of the e-passport network infrastructure. Scalability ensures that the current e-passport system reflects all changes in a timely manner and without performance penalties. For example, suppose that a new international airport has opened. Previous facilities must recognize the airport's new control points, and all control points in the new airport must have access to all passport repositories.

In addition to robust network support, successful verification processes depend on effective support from the passport repository and a reliable access-control system. E-passport systems also require strong government support. If biometric and text information is recorded together in one IC card, the system can't verify travelers' identities when the passports are lost or stolen.

We propose an e-passport mechanism that separates travelers' biometric information from their IC cards. If such a mechanism were implemented, travelers could stop worrying about lost or stolen passports. One of the most important concerns, the privacy of e-passports, is a subject for another article. ■

Jianming Yong *is a senior lecturer at the University of Southern Queensland's School of Information Systems. Contact him at yongj@usq.edu.au.*

Elisa Bertino *is a professor of computer science at Purdue University and research director of Purdue's Center for Education and Research in Information Assurance and Security. Contact her at bertino@cs.purdue.edu.*

Editor: Jack Cole, US Army Research Laboratory's Information Assurance Center, jack.cole@ieee.org; http://msstc.org/cole